Remarks/Arguments

Claims 1-27 remain in the case. Claims 1-27 are rejected. Claims 1-27 remain in this application as originally filed.

Examiner has rejected claims 1-27 under 35 U.S.C. 102 as being anticipated by Borza (US patent #5,995,630). The invention described by the Borza prior art relates to a somewhat different device than the one described with reference to the present application. The problem addressed by the instant invention is described in paragraph 39 of the application. Specifically,

> "In order to breach security of a computer provided with a device according to Fig. 1, a recorder is inserted between the device and the monitor and records a signal provided from the biometric input sensor to the monitor. The recorded signal is then played back to a security access system whenever access to the system is desired."

Refererring to paragraph 40,

> "Referring to Fig. 2, a method is shown for increasing security when using a biometric input sensor with a personal computer. The method according to the invention increases security by authenticating the biometric input sensor as an authorised sensor. Authorised sensors are, for example, biometric input sensors provided from a trusted source such as the manufacturer of the sensor or a verification authority such as Verisign™ certifying the authenticity of the sensor."

In the prior art of Borza (column 4, lines 61-67) the data provided by the sensor is entirely dependent upon, "...means for process the fingerprint image to provide associated data; means for encoding the associated data into an image frame; and, means for providing the image frame comprising the associated data to the computer." While a person of ordinary skill in the art will appreciate that variations in the way a fingerprint is swiped will affect output data from a fingerprint sensor, it is clear that the quoted passage makes no mention

of verifying the authenticity of the fingerprint sensor itself. In this way, the system according to Borza is potentially insecure if, for example, a record of a flow of data from the sensor is recorded and replayed in an attempt to "impersonate" a valid user authentication. A person of skill in the art will appreciate that a system that authenticates the biometric sensor, as described with reference to independent claims 1, 16 and 24, is preferably designed to avoid this security flaw.

Referring to independent claim 1, the following limitation is recited (with underlining for emphasis),

> "...within the biometric information sensor, encoding a value within the digital data, the encoded value related to the digital data and determined in accordance with a known method unique to biometric information sensors approved by a same source and indicative of the same source; and,
> providing the digital data with the encoded value therein from the biometric information sensor to a computer, the digital data absent the encoded value sufficient for determining the encoded value therefrom, wherein a comparison between the encoded value and another value determined according to the known method is suitable for identifying the biometric information sensor as approved by the same source."

Specifically, since the encoded value is provided "indicative of the same source", it is apparent that the encoded value will be indicative of the source (in this case a biometric sensor, as recited in the preamble of claim 1). Thus, the sensor itself is authenticated thereby providing an additional layer of security.

Independent claim 16 recites,

> "...within the biometric information sensor, determining a value indicative of a unique source of the biometric information sensor according to the method of determining a value;

within the biometric information sensor, encoding the value indicative of the biometric information sensor according to the method of encoding a value..."

Additionally, independent claim 24 recites,

"...identifying the biometric information sensor to the computer as an authorised biometric information sensor, the information derived in accordance with a verifiable method wherein verification of the method is indicative of the biometric information sensor being an authorised biometric information sensor..."

Such identification of a sensor is not present in the prior art of Borza. With this in mind, it is apparent that the prior art of Borza does not teach the essential features of the invention as recited in independent claims 1, 16 and 24 and therefore it is apparent that claims 1, 16 and 24 are not anticipated by Borza. Further, the prior art of Borza does not teach or suggest a system in which a "biometric sensor" is authenticated. The prior art system of Borza is focused on authenticating a user, not a sensor. Thus, a person of ordinary skill in the art of securing systems having reviewed Borza would not be lead to the system as described in independent claims 1, 16 and 24. With this in mind, it is apparent that independent claims 1, 16 and 24 are neither anticipated nor obvious in light of the prior art of Borza.

Claims 2-15, 17-23 and 25-27 depend either directly or indirectly from independent claims 1, 16 and 24. Since independent claims 1, 16 and 24 are neither anticipated nor obvious, dependent claims 2-15, 17-23 and 25-27 cannot be anticipated or obvious.

No new matter has been added in the amended claims.

Applicant looks forward to favourable reconsideration of the present application.

Please charge any additional fees required or credit any overpayment to Deposit Account No: 50-1142.

Respectfully submitted,

Gordon Freedman, Reg. No. 41,553

Freedman and Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel: (613) 274-7272
Fax: (613) 274-7414
Email: gordon@ipatent4u.com

GF/VL/bh